

**Method and Device for Calculating a Result of an  
Exponentiation**

5

ABSTRACT

For calculating the result of an exponentiation  $B^d$ ,  $B$  being a base and  $d$  being an exponent which can be described by a binary number from a plurality of bits, a first auxiliary quantity  $X$  is at first initialized to a value of 1. Then a  
10 second auxiliary quantity  $Y$  is initialized to the base  $B$ . Then, the bits of the exponent are sequentially processed by updating the first auxiliary quantity  $X$  by  $X^2$  or by a value derived from  $X^2$  and by updating the second auxiliary quantity  $Y$   
15 by  $X*Y$  or by a value derived from  $X*Y$ , if a bit of the exponent equals 0. If a bit of the exponent equals 1, the first auxiliary quantity  $X$  is updated by  $X*Y$  or by a value derived from  $X*Y$  and the second auxiliary quantity  $Y$  is updated by  $Y^2$  or by a value derived from  $Y^2$ . After sequentially  
20 processing all the bits of the exponent, the value of the first auxiliary quantity  $X$  is used as the result of the exponentiation. Thus a higher degree of security is obtained by homogenizing the time and current profiles. In addition, an increase in performance is enabled by a possible parallel  
25 performance of operations.

Figure 1